What is claimed is:

1 1. An encryption method for use by an encryption apparatus

2 that encrypts plaintext data composed of a plurality of

3 blocks, the encryption method comprising:

4   a block obtaining step for obtaining the plaintext

5 data one block at a time in order from outside the

6 encryption apparatus;

7   a selecting step for selecting either a first mode

8 or a second mode for a current block obtained in the block

9 obtaining step according to how many blocks have been

10 obtained;

11   a key generating step for generating

12   (1) a first group composed of a predetermined

13   number n of different subkeys when the first

14   mode is selected, and

15   (2) a second group composed of less than n

16   different subkeys when the second mode is

17   selected; and

18   an encrypting step for encrypting the current block

19 by subjecting the current block to n conversion processes

20 in order, wherein

21   in the first mode, each of the n conversion processes

22 is associated with a different subkey in the first group

23 and is performed using the associated subkey, and

24   in the second mode, the n conversion processes are

25 associated with subkeys in the second group and are each

26 performed using the associated subkey.

1   2. An encryption method according to Claim 1,

2   wherein the selecting step selects

3   (i) the first mode for blocks whenever a number

4   of blocks that have been obtained is equal to

5   a multiple of a predetermined value, and

6   (ii) the second mode for all other cases.

1   3. An encryption method according to Claim 1,

2   wherein the encryption apparatus includes an initial

3   value storing means for storing an initial value,

4   the encrypting step encrypts the current block to

5   generate a ciphertext block having a predetermined length,

6   and

7   the key generating step generates the first group

8   using the initial value in the first mode and generates

9   the second group using the initial value and the ciphertext

10   block most recently generated by the encrypting step in

11   the second mode.

1   4. An encryption apparatus for encrypting plaintext data

2   composed of a plurality of blocks, the encryption apparatus

3   comprising:

4   block obtaining means for obtaining the plaintext

5   data one block at a time in order from outside;

6   selecting means for selecting either a first mode or

7   a second mode for use with a current block obtained in the

8   block obtaining means according to how many blocks have

58

9   been obtained;

10   key generating means for generating

11   (1) a first group composed of a predetermined

12   number n of different subkeys when the first

13   mode is selected, and

14   (2) a second group composed of less than n

15   different subkeys when the second mode is

16   selected; and

17   encrypting means for encrypting the current block by

18   subjecting the current block to n conversion processes in

19   order, wherein

20   in the first mode, each of the n conversion processes

21   is associated with a different subkey in the first group

22   and is performed using the associated subkey, and

23   in the second mode, the n conversion processes are

24   each associated with a subkey in the second group and are

25   each performed using the associated subkey.

1   5. A computer-readable storage medium storing an

2   encryption program for use by a computer that encrypts

3   plaintext data composed of a plurality of blocks,

4   the encryption program comprising:

5   a block obtaining step for obtaining the plaintext

6   data one block at a time in order from outside the

7   encryption apparatus;

8   a selecting step for selecting either a first mode

9   or a second mode for a current block obtained in the block

10   obtaining step according to how many blocks have been

11   obtained;

12   a key generating step for generating

13   (1) a first group composed of a predetermined

14   number n of different subkeys when the first

15   mode is selected, and

16   (2) a second group composed of less than n

17   different subkeys when the second mode is

18   selected; and

19   an encrypting step for encrypting the current block

20   by subjecting the current block to n conversion processes

21   in order, wherein

22   in the first mode, each of the n conversion processes

23   is associated with a different subkey in the first group

24   and is performed using the associated subkey, and

25   in the second mode, the n conversion processes are

26   associated with subkeys in the second group and are each

27   performed using the associated subkey.

1   6. A decryption method for use by a decryption apparatus

2   that decrypts ciphertext data in ciphertext block units,

3   the decryption method comprising:

4   a block obtaining step for obtaining the ciphertext

5   data one ciphertext block at a time in order from outside

6   the decryption apparatus;

7   a selecting step for selecting either a first mode

8   or a second mode for use with a current ciphertext block

9   obtained in the block obtaining step according to how many

10   ciphertext blocks have been obtained;

11   a key generating step for generating

12   (1) a first group composed of a predetermined

13   number n of different subkeys when the first

14   mode is selected and

15   (2) a second group composed of less than n

16   different subkeys when the second mode is

17   selected; and

18   a decrypting step for decrypting the current

19   ciphertext block by subjecting the current ciphertext

20   block to n conversion processes in order, wherein

21   in the first mode, each of the n conversion processes

22   is associated with a different subkey in the first group

23   and is performed using the associated subkey, and

24   in the second mode, the n conversion processes are

25   associated with subkeys in the second group and are each

26   performed using the associated subkey.

1   7. A decryption method according to Claim 6,

2   wherein the selecting step selects

3   (1) the first mode whenever a number of

4   ciphertext blocks that have been obtained is

5   given as a multiple of a predetermined value,

6   and

7   (2) the second mode for all other cases.

1   8. A decryption method according to Claim 6,

2   wherein the decryption apparatus includes an initial

3 value storing means for storing an initial value,

4   the key generating step generating the first group

5 using the initial value in the first mode and generating

6 the second group using the initial value and the ciphertext

7 block obtained immediately before the current ciphertext

8 block in the second mode.

1   9. A decryption apparatus that decrypts ciphertext data

2 in ciphertext block units, the decryption apparatus

3 comprising:

4   block obtaining means for obtaining the ciphertext

5 data one ciphertext block at a time in order from outside;

6   selecting means for selecting either a first mode or

7 a second mode for use with a current ciphertext block

8 obtained by the block obtaining means according to how many

9 ciphertext blocks have been obtained;

10   key generating means for generating

11   (1) a first group composed of a predetermined

12   number n of different subkeys when the first

13   mode is selected, and

14   (2) a second group composed of less than n

15   different subkeys when the second mode is

16   selected; and

17   decrypting means for decrypting the current

18 ciphertext block by subjecting the current ciphertext

19 block to *n* conversion processes in order, wherein

20   in the first mode, each of the *n* conversion processes

21 is associated with a different subkey in the first group

22 and is performed using the associated subkey, and

23   in the second mode, the *n* conversion processes are

24 associated with subkeys in the second group and are each

25 performed using the associated subkey.

1   10. A computer-readable storage medium storing a

2   decryption program for use by a computer that decrypts

3   ciphertext data in ciphertext block units,

4   the decryption program comprising:

5   a block obtaining step for obtaining the ciphertext

6   data one ciphertext block at a time in order from outside

7   the decryption apparatus;

8   a selecting step for selecting either a first mode

9   or a second mode for use with a current ciphertext block

10 obtained in the block obtaining step according to how many

11 ciphertext blocks have been obtained;

12   a key generating step for generating

13   (1) a first group composed of a predetermined

14   number *n* of different subkeys when the first

15   mode is selected and

16   (2) a second group composed of less than *n*

17   different subkeys when the second mode is

18   selected; and

19   a decrypting step for decrypting the current

20 ciphertext block by subjecting the current ciphertext

21 block to n conversion processes in order, wherein

22   in the first mode, each of the n conversion processes

23 is associated with a different subkey in the first group

24 and is performed using the associated subkey, and

25   in the second mode, the n conversion processes are

26 associated with subkeys in the second group and are each

27 performed using the associated subkey.